Exam. Code: 1046
Sub. Code: 35462

2055

M.E. (Computer Science and Engineering - Cyber Security)
Second Semester
CSN-8206: Internet of Things Security

Time allowed: 3 Hours Max. Marks: 50

NOTE: *Attempt five questions in all, including Question No. I which is compulsory and selecting two questions from each Unit.*

1. Attempt the following:-
   a) Define the IoT security life cycle.
   b) Outline the process of data collection in IoT systems.
   c) What is threat modeling in the context of IoT security?
   d) Name any two cryptographic algorithms used in IoT.
   e) How can one build security in design and development?
   f) Why is mapping wireless IoT networks important for attackers?
   g) Justify the role of biometrics in enhancing security for IoT systems.
   h) What is provisioning in the IoT Security Life Cycle?
   i) How do AWS and Azure secure communication between IoT devices and the cloud?
   j) What is the primary role of an Identity Provider (IdP) in IoT IAM infrastructure? (10x1)

UNIT - I

2. Explain the role of different network layers in an IoT enterprise architecture. Describe common protocols used at the physical, data link, and application layers. (10)

3. What are the major security challenges in terms of attacks and vulnerabilities in deploying IoT systems? Enlist few countermeasures for these attacks. (10)

4. Explain the different phases of the IoT Security Life Cycle and their significance in maintaining a secure IoT environment. (10)

P.T.O.

UNIT - II

5. Compare symmetric and asymmetric key cryptography. How are both used in securing IoT devices and communication? (10)
6. Discuss the cryptographic controls built into IoT communication protocols an IoT messaging protocols. (10)
7. Explain the concept of the identity lifecycle in IoT. Describe each stage and its role in maintaining secure device identity. (10)

x-x-x